Table of Contents

1 Checkpoint Integration

PINsafe to Checkpoint Gaia

Integration Notes

2 Overview

Swivel can provide strong and two factor authentication to the Checkpoint Gaia. This document outlines the details required to carry this out.

3 Baseline

Swivel 4.x

Checkpoint Gaia appliance version R77.30.

4 Prerequisites

Working Checkpoint, smart console

Swivel 4.x

Note that modifications to the Connectra login page will affect ALL users (but not the administration page).

Use of the TURing, Security String Index or SMS Confirmed message will require the use of a NAT.

When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

5 Gaia Configuration

5.1 Enabling RADIUS Authentication in Gaia

You need to configure Swivel as an authentication server on the Gaia appliance.

- Open Smart Dashboard and log in.
- Under Network and Resources -> Hosts, configure the Swivel server as a new host. You just need to give it a name and add the IP address.
- Under Users and Authentication -> Authentication -> RADIUS Servers, create a new RADIUS server. Select Swivel as the host, ?NEW-RADIUS? as the service, and enter the shared secret you previously set on the Swivel server. You can select RADIUS version 1 or 2, and PAP or MSChap as the protocol: Swivel will detect these protocols automatically. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

You will also need to configure authentication for the relevant users. The simplest way to handle this is to create a new user group containing all users that will be using Swivel (if you do not already have one):

- Go to Users and Authentication -> Internal Users -> User Groups.
- Then under User Templates, create a new template, or modify an existing one, containing the relevant group, and set the authentication to RADIUS, using the Swivel server.

Don?t forget to save and install the policy once you have made all relevant changes.

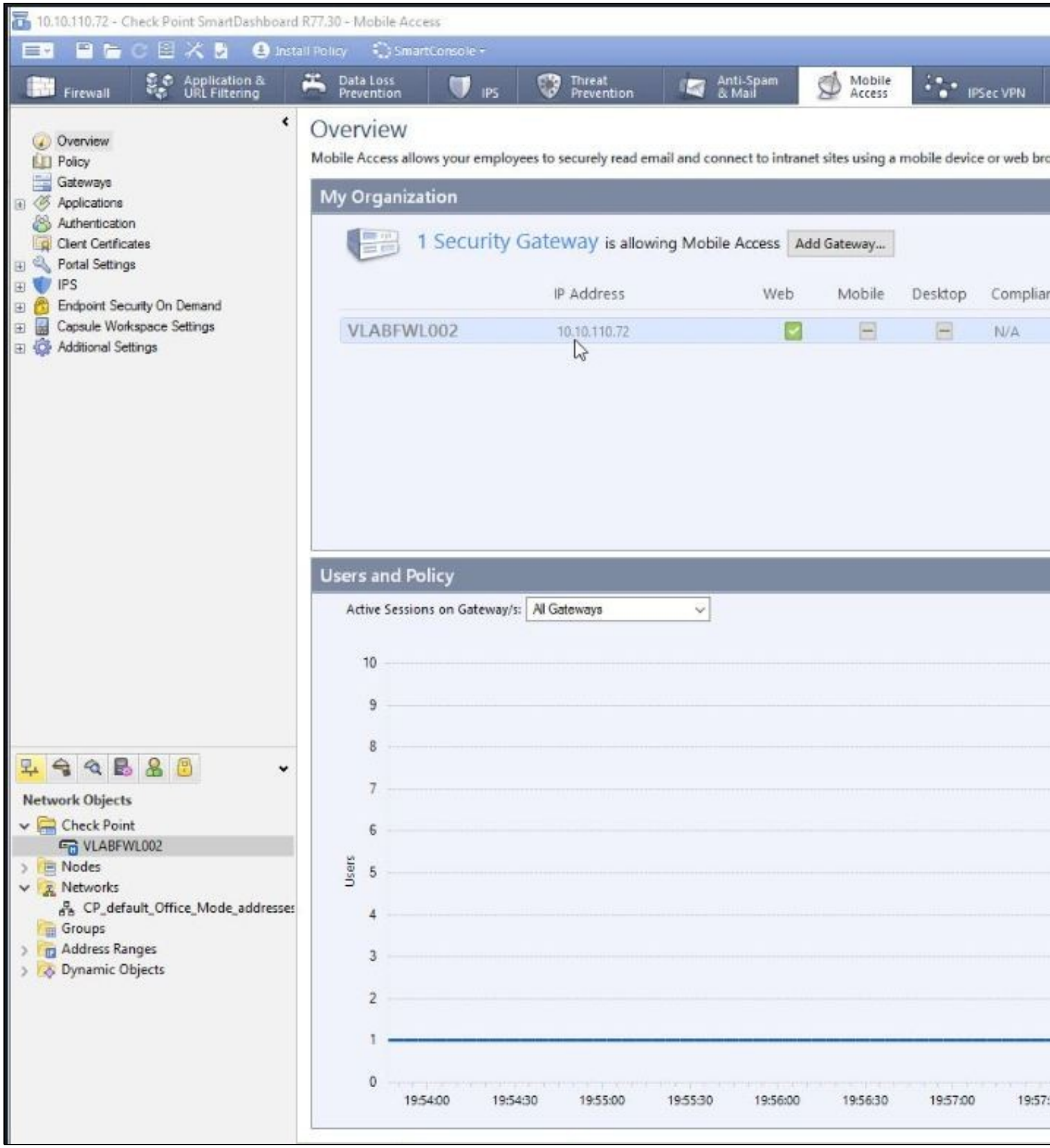
6 Customising the Gaia Login Page

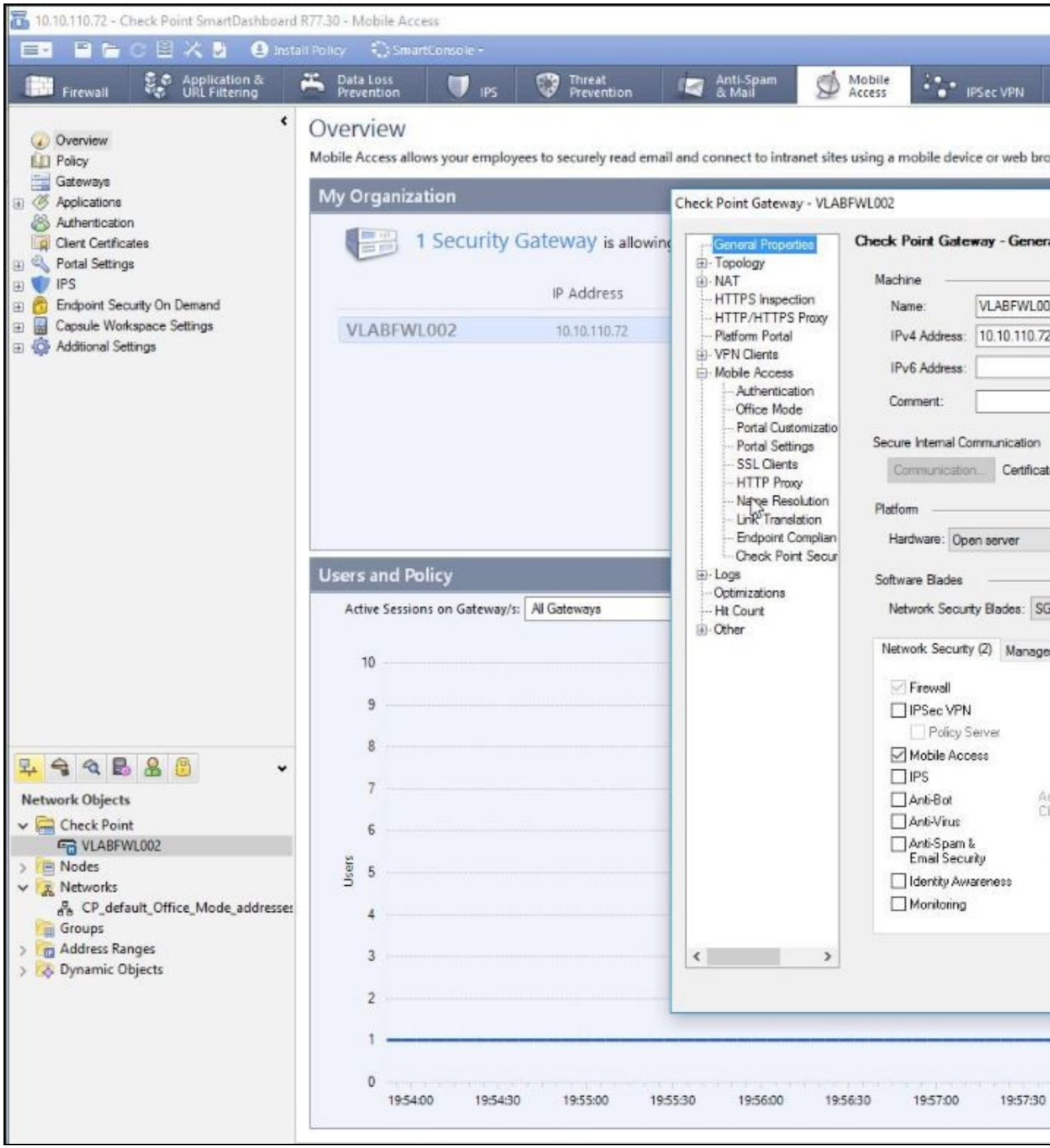
NOTE: it is assumed here that you are familiar with Unix commands, in particular with the vi editor, as you will need to edit a file.

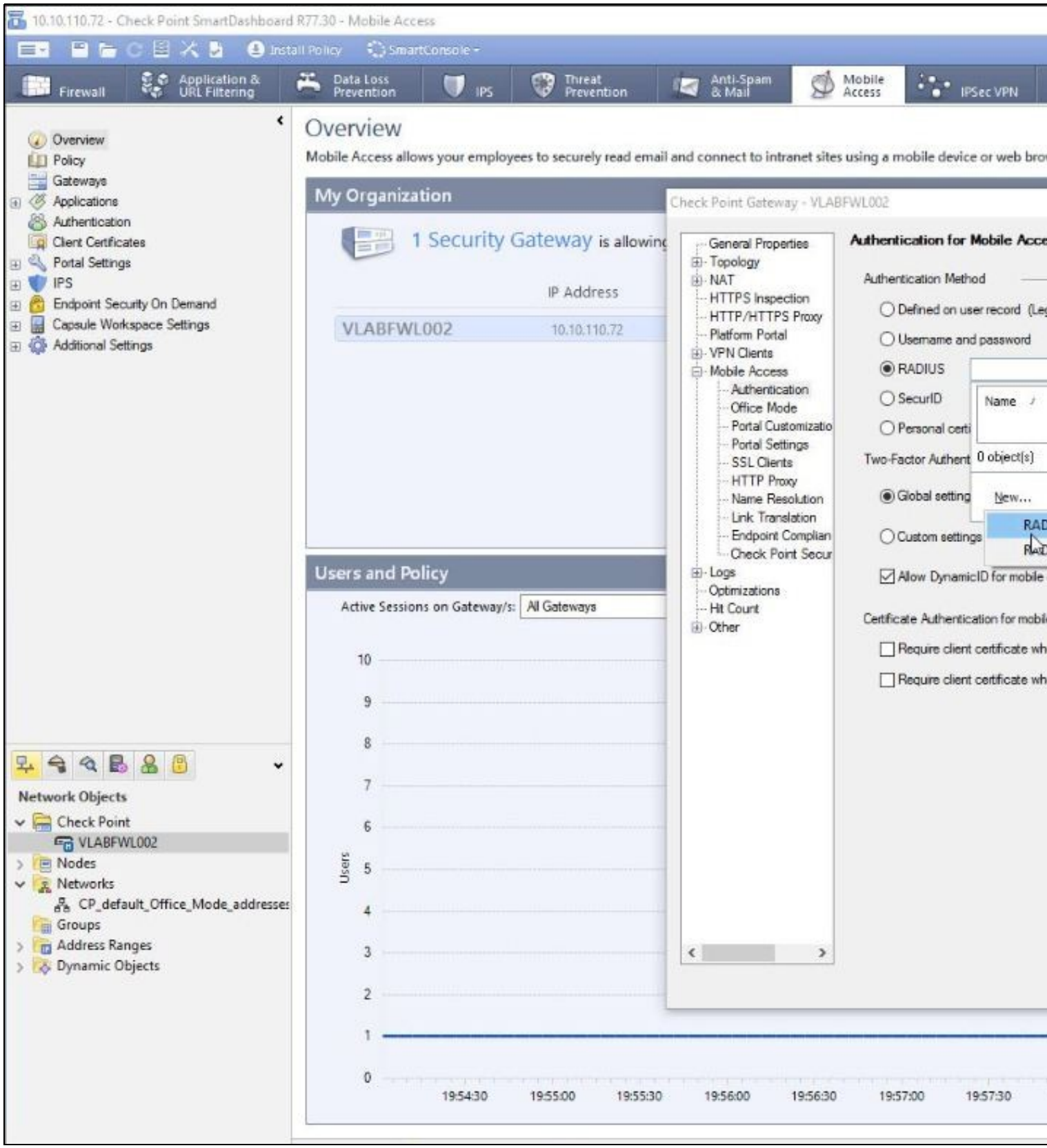
NOTE: There is an example LoginPage.php available which is the Login.php file with the modifications already included. This can be used for reference but may not be 100% suitable for specific installations and different Gaia versions.

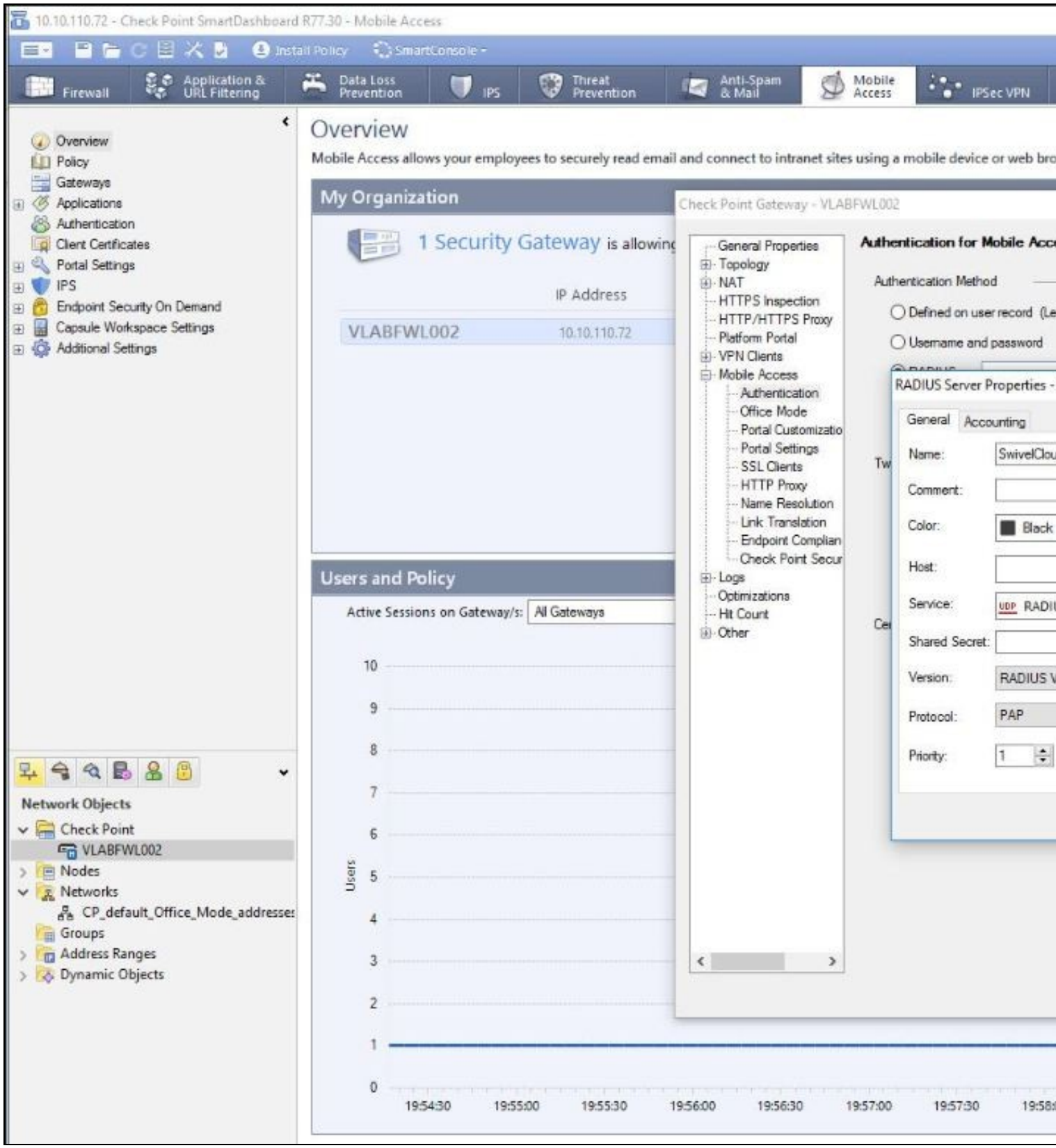
6.1 Test the RADIUS authentication

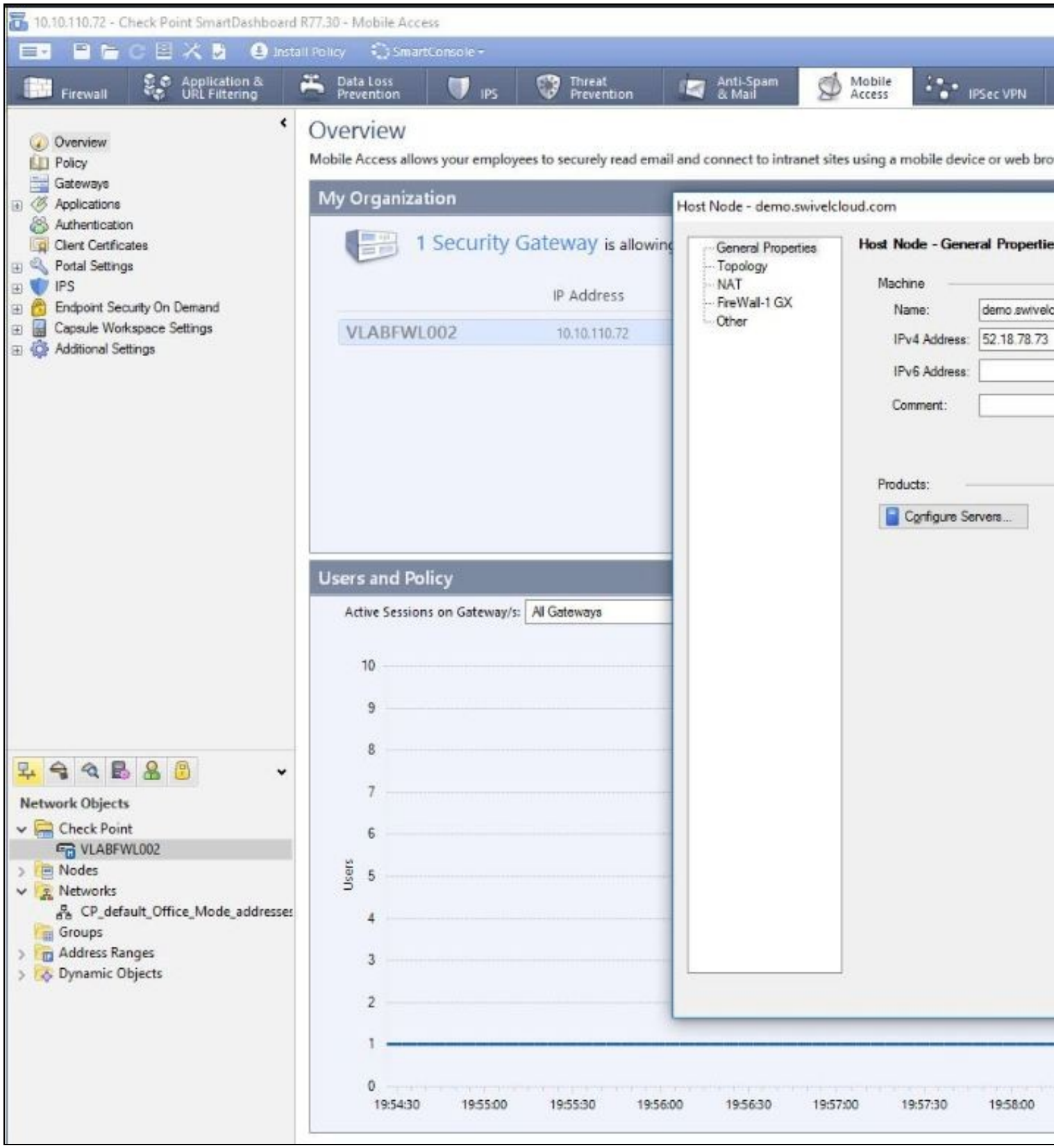
At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

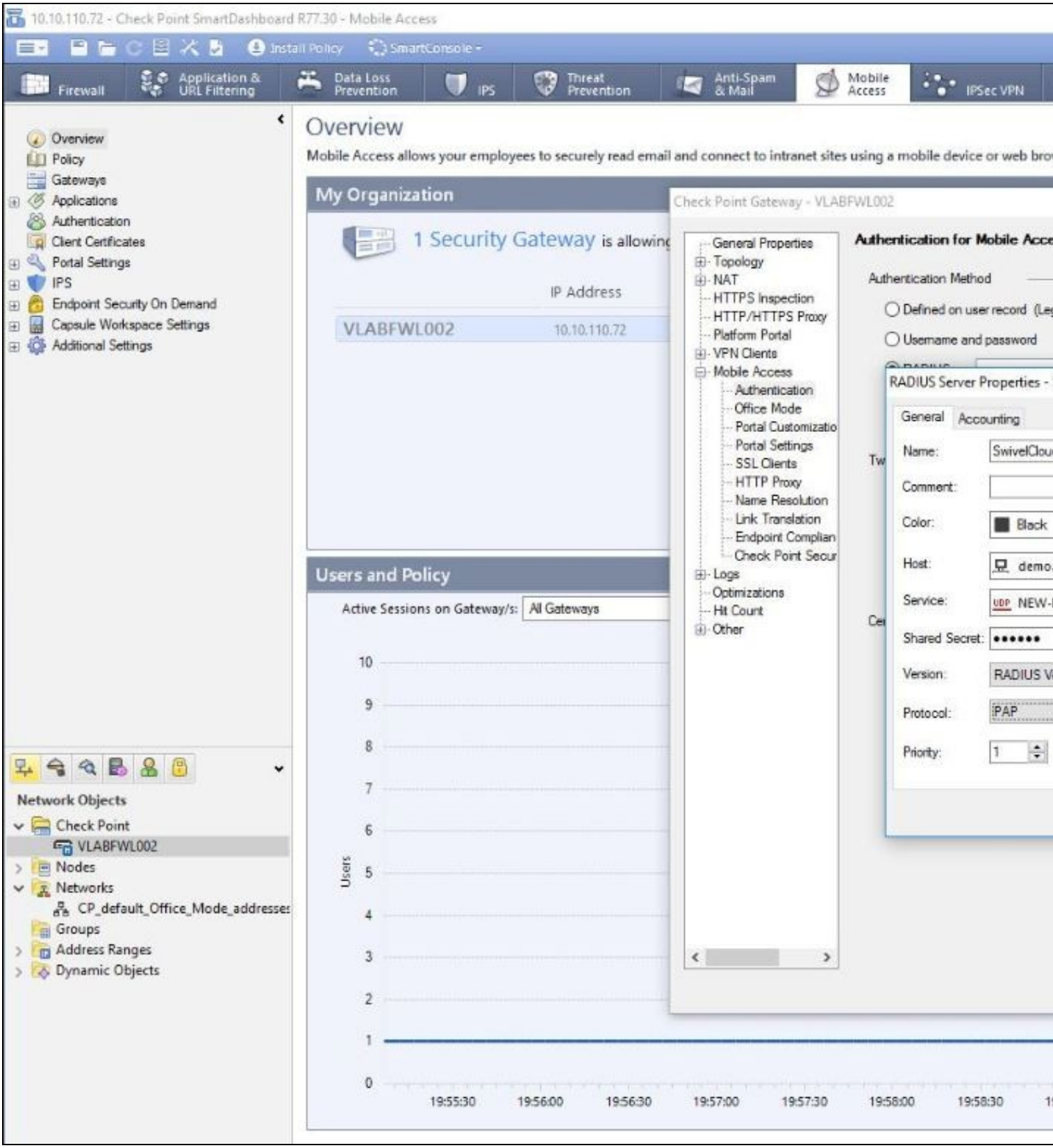

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web br
My Organization
1 Security Gateway is allowing Mobile Access
Add Gateway...
IP Address
Web
Mobile
Desktop
Compliar
VLABFWL002
10.10.110.72
N/A
Users and Policy
Active Sessions on Gateway/s:
All Gateways
10
9
8
7
6
5
4
3
2
1
0
Users
19:54:00
19:54:30
19:55:00
19:55:30
19:56:00
19:56:30
19:57:00
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects

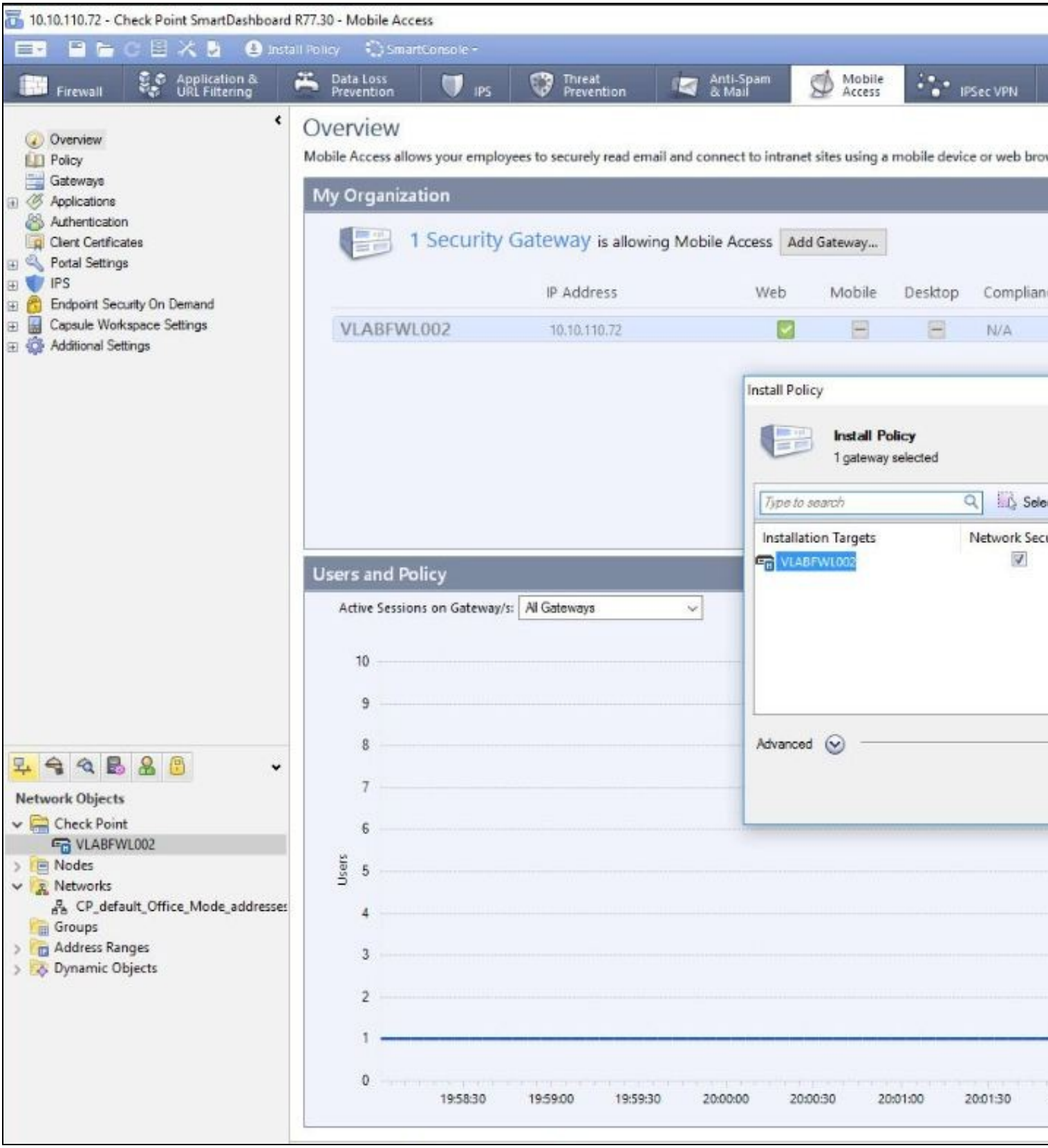

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowin
IP Address
VLABFWL002
10.10.110.72
Check Point Gateway - VLABFWL002
General Properties
Topology
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
VPN Clients
Mobile Access
Authentication
Office Mode
Portal Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Check Point Gateway - Gener
Machine
Name:
VLABFWL00
IPv4 Address:
10.10.110.72
IPv6 Address:
Comment:
Secure Internal Communication
Communication...
Certificat
Platform
Hardware:
Open server
Software Blades
Network Security Blades:
SG
Network Security (2)
Manage
Firewall
IPSec VPN
Policy Server
Mobile Access
IPS
Anti-Bot
Anti-Virus
Anti-Spam & Email Security
Identity Awareness
Monitoring
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:54:00
19:54:30
19:55:00
19:55:30
19:56:00
19:56:30
19:57:00
19:57:30
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects

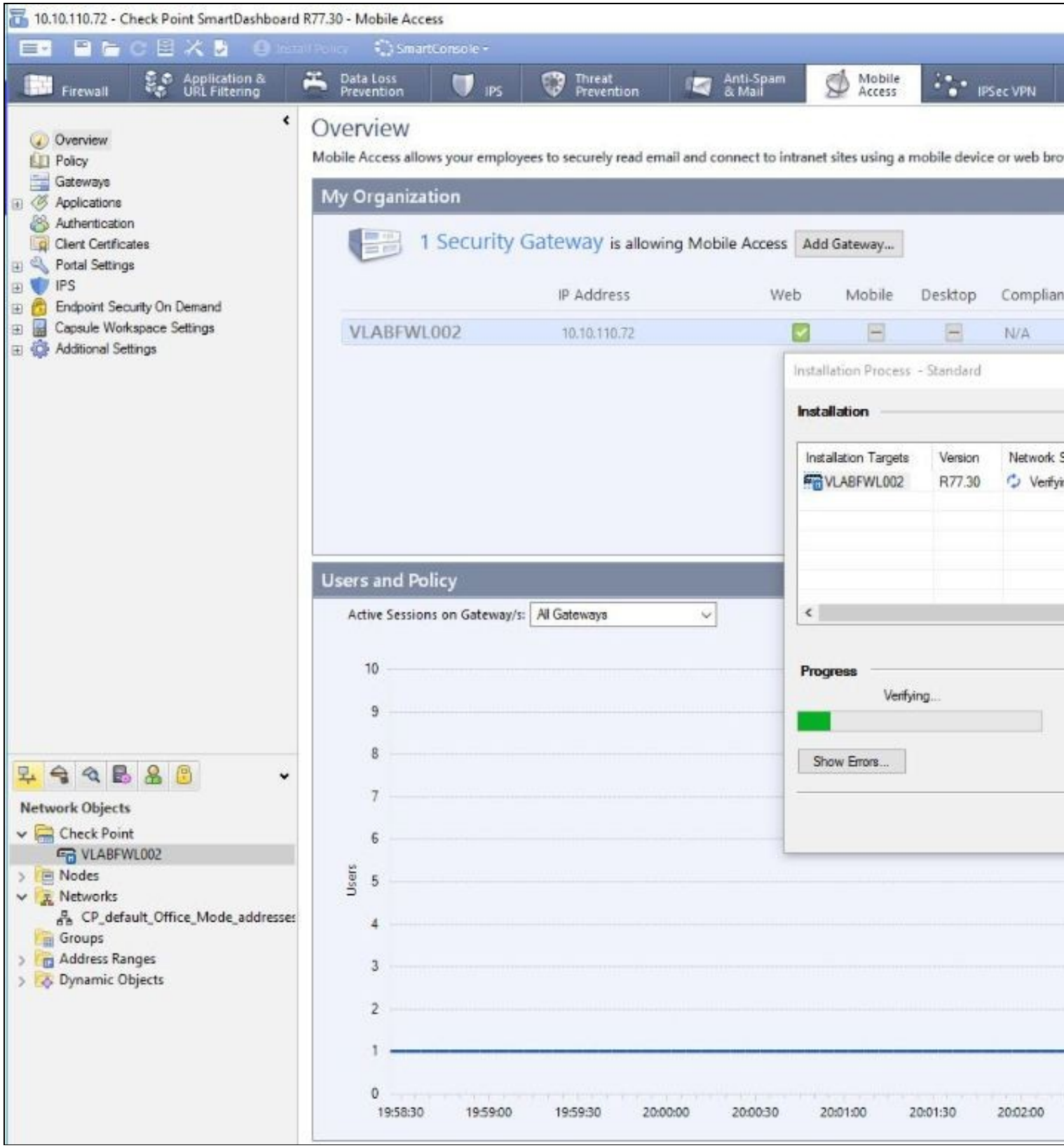

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing
IP Address
VLABFWL002
10.10.110.72
Check Point Gateway - VLABFWL002
General Properties
Topology
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
VPN Clients
Mobile Access
Authentication
Office Mode
Portal Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Acce
Authentication Method
Defined on user record (Leg
Username and password
RADIUS
SecurID
Personal certi
Name
Two-Factor Authent
0 object(s)
Global setting
New...
Custom settings
Allow DynamicID for mobile
Certificate Authentication for mobil
Require client certificate wh
Require client certificate wh
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:54:30
19:55:00
19:55:30
19:56:00
19:56:30
19:57:00
19:57:30
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects

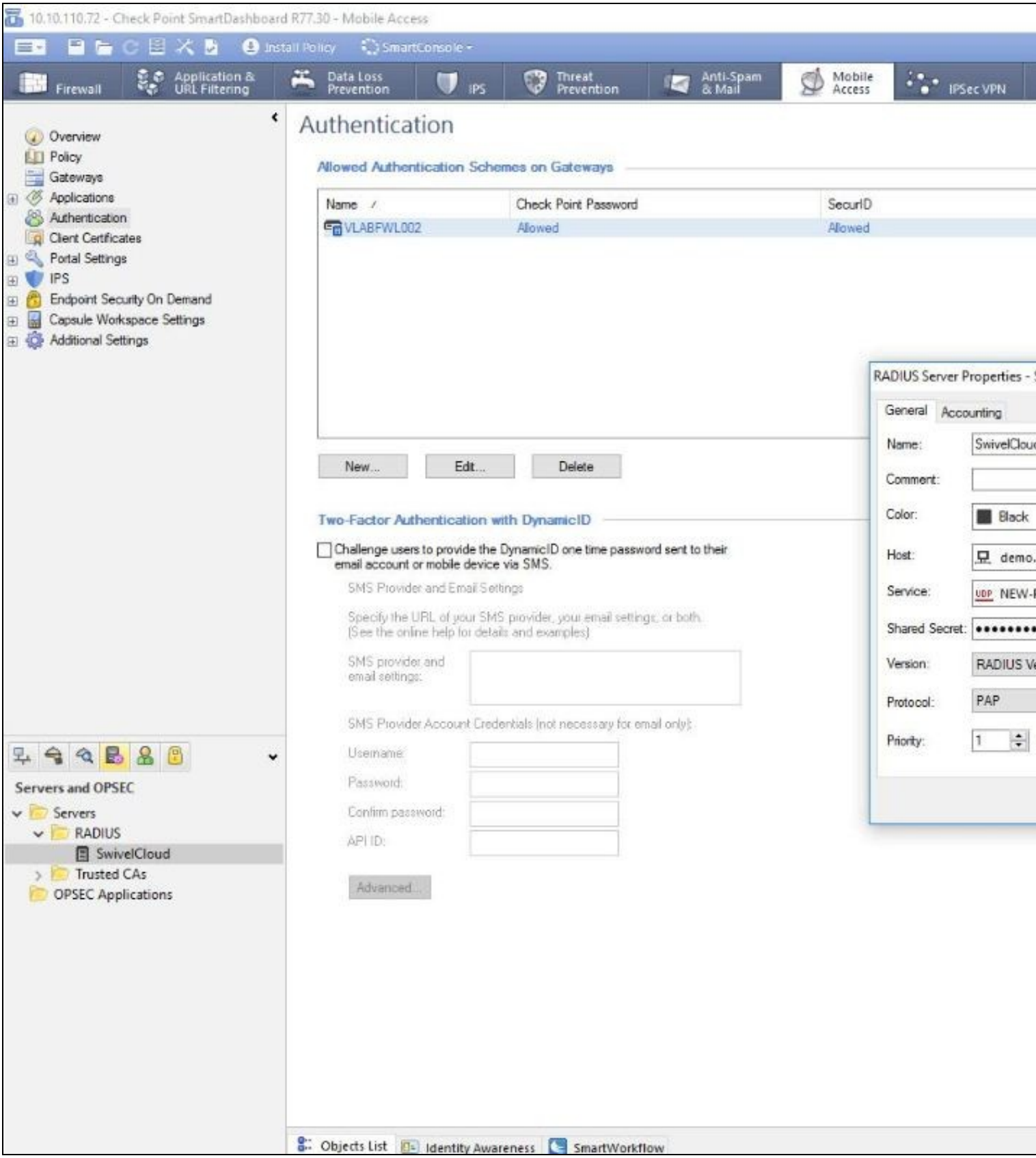

10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing
IP Address
VLABFWL002
10.10.110.72
Check Point Gateway - VLABFWL002
General Properties
Topology
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
VPN Clients
Mobile Access
Authentication
Office Mode
Portal Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Acc
Authentication Method
Defined on user record (Le
Username and password
RADIUS Server Properties -
General
Accounting
Name:
SwivelClou
Comment:
Color:
Black
Host:
Service:
UDP RADIU
Shared Secret:
Version:
RADIUS V
Protocol:
PAP
Priority:
1
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:54:30
19:55:00
19:55:30
19:56:00
19:56:30
19:57:00
19:57:30
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects


10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowin
IP Address
VLABFWL002
10.10.110.72
Host Node - demo.swivelcloud.com
General Properties
Topology
NAT
FireWall-1 GX
Other
Host Node - General Properties
Machine
Name:
demo.swivelc
IPv4 Address:
52.18.78.73
IPv6 Address:
Comment:
Products:
Configure Servers...
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:54:30
19:55:00
19:55:30
19:56:00
19:56:30
19:57:00
19:57:30
19:58:00
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects


10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing
IP Address
VLABFWL002
10.10.110.72
Check Point Gateway - VLABFWL002
General Properties
Topology
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
Platform Portal
VPN Clients
Mobile Access
Authentication
Office Mode
Portal Customizatio
Portal Settings
SSL Clients
HTTP Proxy
Name Resolution
Link Translation
Endpoint Complian
Check Point Secur
Logs
Optimizations
Hit Count
Other
Authentication for Mobile Acce
Authentication Method
Defined on user record
Username and password
RADIUS Server Properties -
General
Accounting
Name:
Comment:
Color:
Black
Host:
Service:
Shared Secret:
Version:
Protocol:
PAP
Priority:
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:55:30
19:56:00
19:56:30
19:57:00
19:57:30
19:58:00
19:58:30
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects


10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing Mobile Access
Add Gateway...
IP Address
Web
Mobile
Desktop
Complian
VLABFWL002
10.10.110.72
N/A
Install Policy
Install Policy
1 gateway selected
Type to search
Installation Targets
Network Sec
VLABFWL002
Advanced
Users and Policy
Active Sessions on Gateway/s:
All Gateways
10
9
8
7
6
5
4
3
2
1
0
Users
19:58:30
19:59:00
19:59:30
20:00:00
20:00:30
20:01:00
20:01:30
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects


10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Overview
Mobile Access allows your employees to securely read email and connect to intranet sites using a mobile device or web bro
My Organization
1 Security Gateway is allowing Mobile Access
Add Gateway...
IP Address
Web
Mobile
Desktop
Complian
VLABFWL002
10.10.110.72
N/A
Installation Process - Standard
Installation
Installation Targets
Version
Network S
VLABFWL002
R77.30
Verifyi
Progress
Verifying...
Show Errors...
Users and Policy
Active Sessions on Gateway/s:
All Gateways
Users
10
9
8
7
6
5
4
3
2
1
0
19:58:30
19:59:00
19:59:30
20:00:00
20:00:30
20:01:00
20:01:30
20:02:00
Network Objects
Check Point
VLABFWL002
Nodes
Networks
CP_default_Office_Mode_addresses
Groups
Address Ranges
Dynamic Objects


10.10.110.72 - Check Point SmartDashboard R77.30 - Mobile Access
Install Policy
SmartConsole
Firewall
Application & URL Filtering
Data Loss Prevention
IPS
Threat Prevention
Anti-Spam & Mail
Mobile Access
IPSec VPN
Overview
Policy
Gateways
Applications
Authentication
Client Certificates
Portal Settings
IPS
Endpoint Security On Demand
Capsule Workspace Settings
Additional Settings
Authentication
Allowed Authentication Schemes on Gateways
Name
Check Point Password
SecurID
VLABFWL002
Allowed
Allowed
New...
Edit...
Delete
Two-Factor Authentication with DynamicID
Challenge users to provide the DynamicID one time password sent to their email account or mobile device via SMS.
SMS Provider and Email Settings
Specify the URL of your SMS provider, your email settings, or both. (See the online help for details and examples)
SMS provider and email settings:
SMS Provider Account Credentials (not necessary for email only):
Username:
Password:
Confirm password:
API ID:
Advanced...
RADIUS Server Properties -
General
Accounting
Name:
Comment:
Color:
Black
Host:
Service:
Shared Secret:
Version:
Protocol:
PAP
Priority:
1
Servers and OPSEC
Servers
RADIUS
SwivelCloud
Trusted CAs
OPSEC Applications
Objects List
Identity Awareness
SmartWorkflow

7 Swivel Configuration

7.1 Configuring the RADIUS server

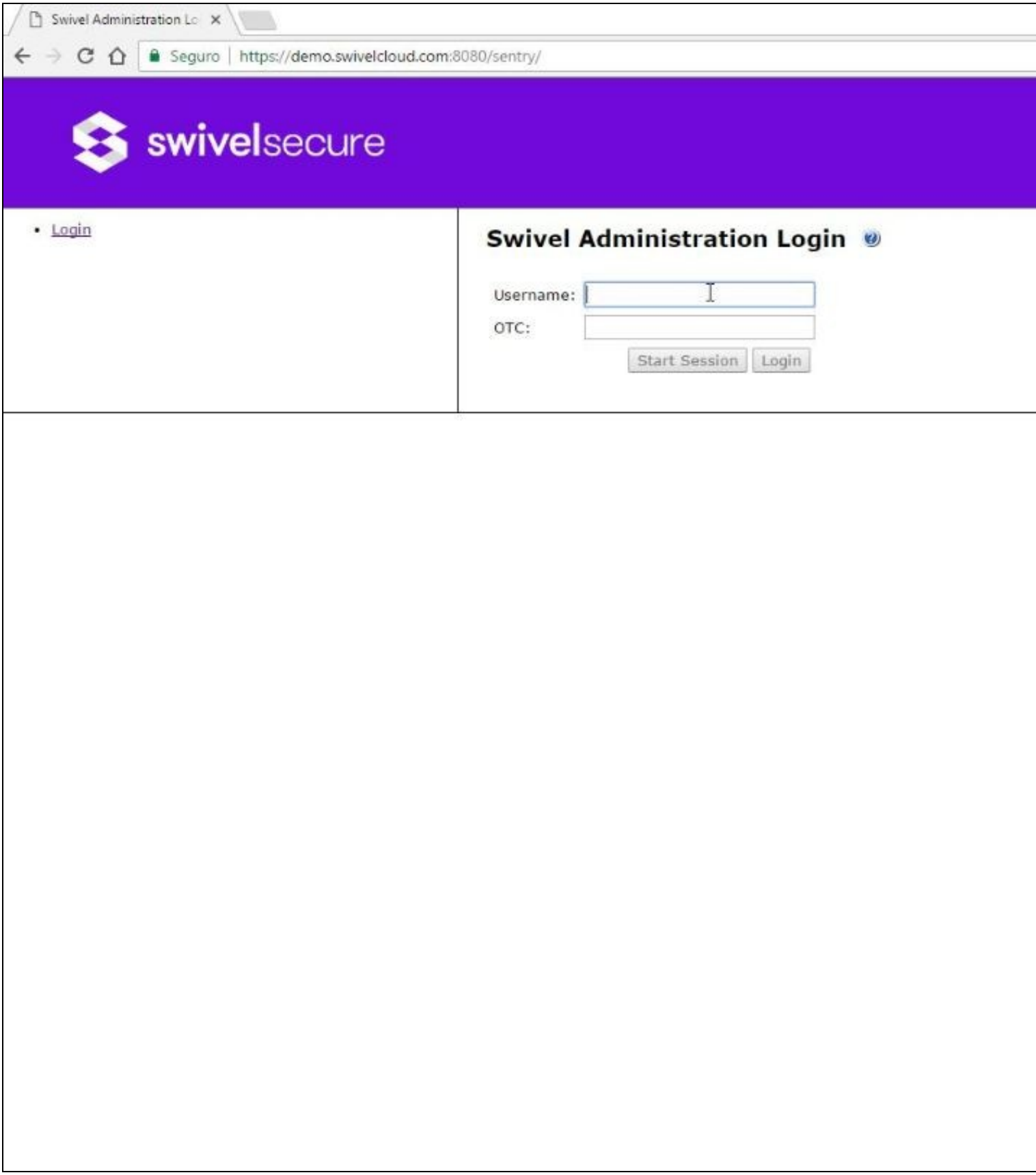
On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

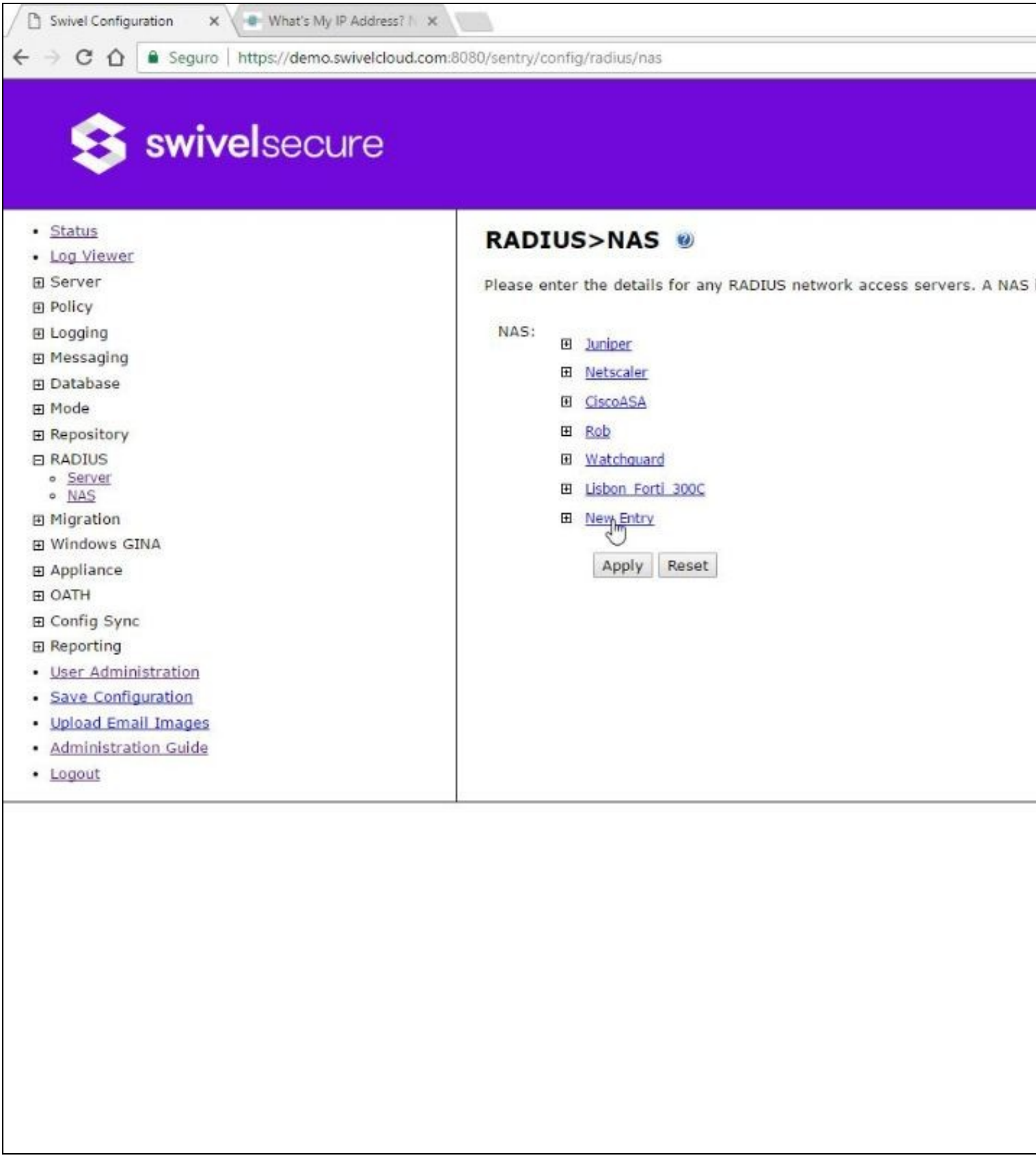
7.2 Enabling Session creation with username

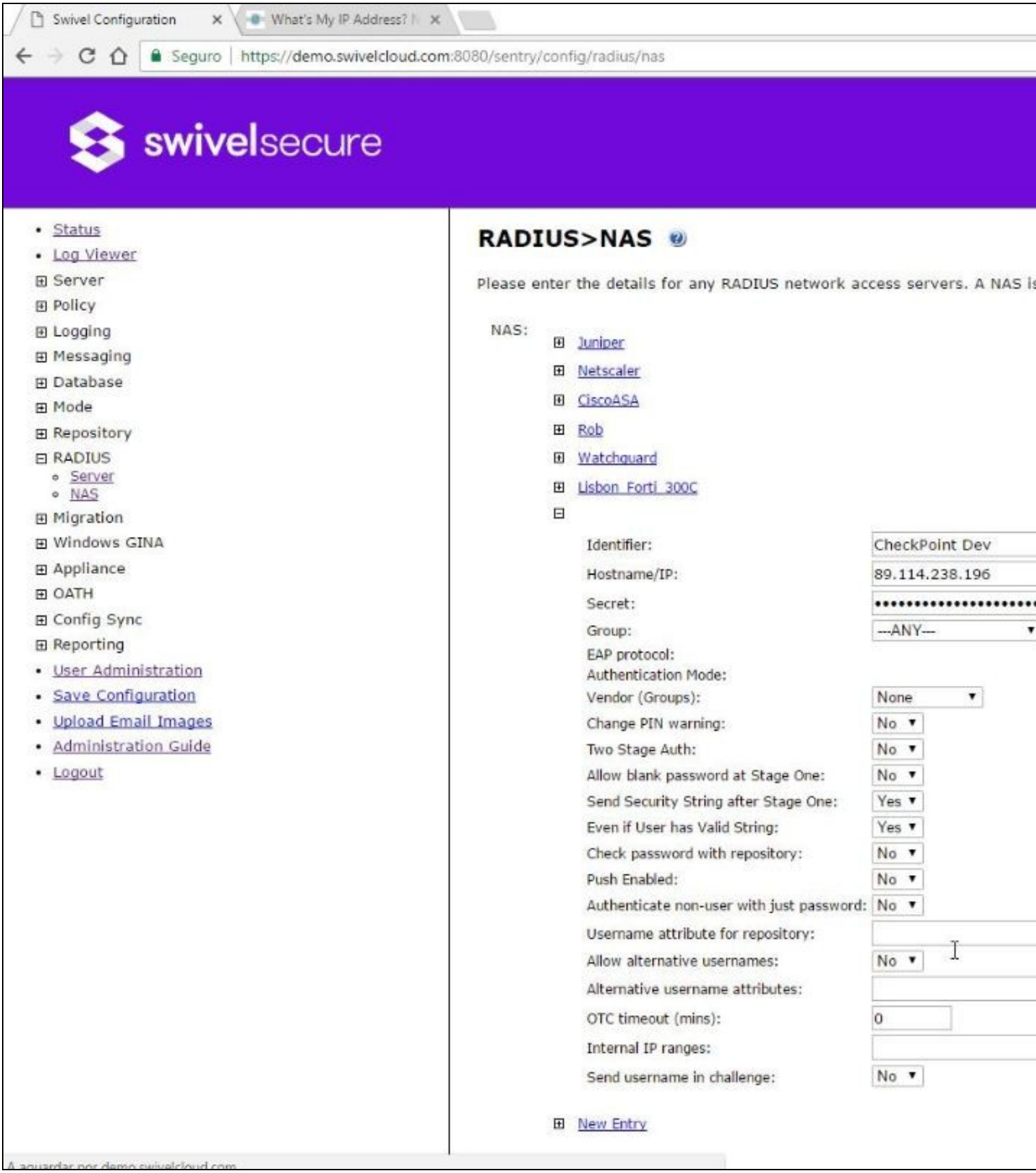
To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

7.3 Setting up Swivel Dual Channel Transports

See Transport Configuration

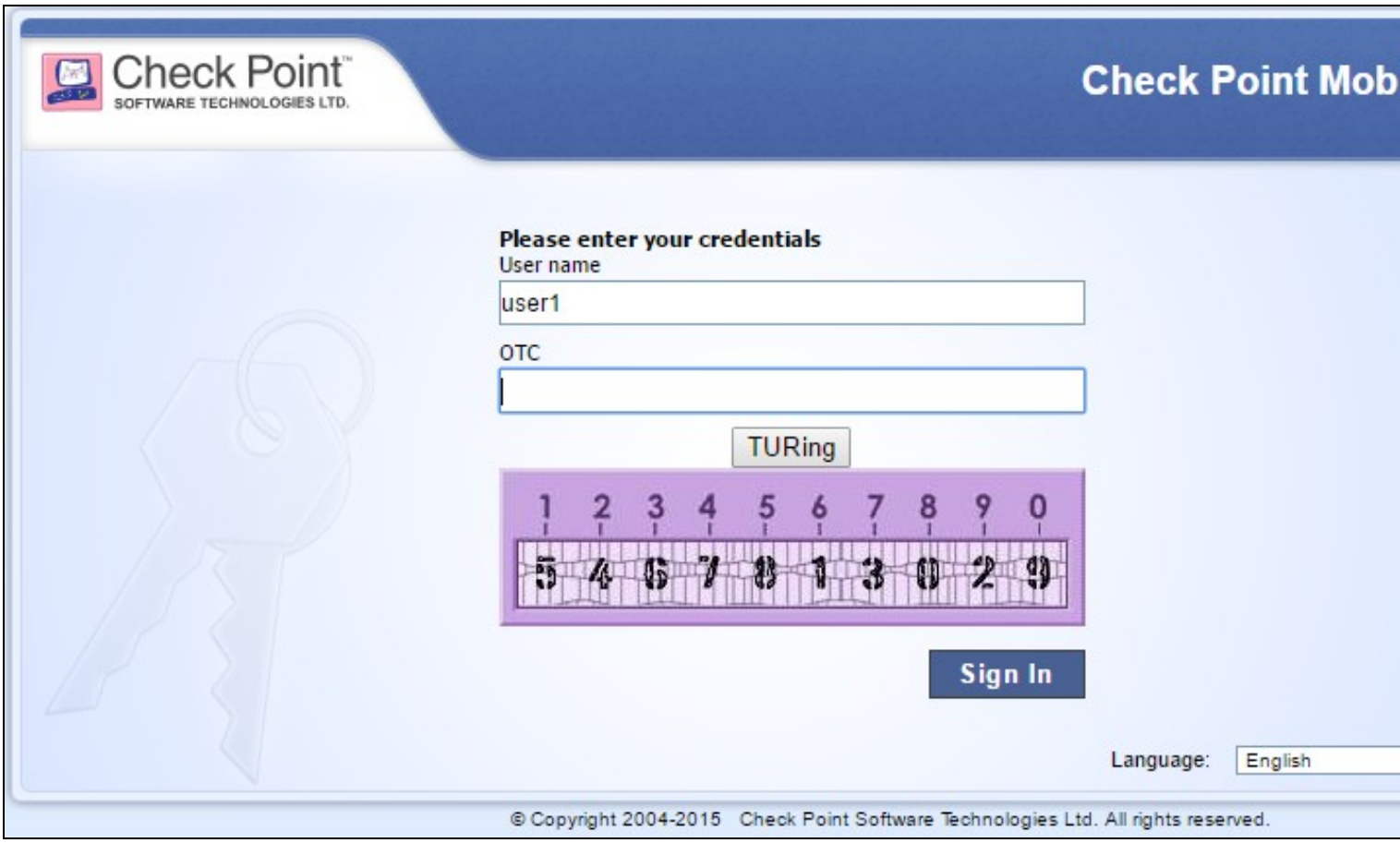

Swivel Administration Lo
Seguro | https://demo.swivelcloud.com:8080/sentry/
swivelsecure
Login
Swivel Administration Login
Username:
OTC:
Start Session
Login


Swivel Configuration
What's My IP Address?
Seguro
https://demo.swivelcloud.com:8080/sentry/config/radius/nas
swivelsecure
Status
Log Viewer
Server
Policy
Logging
Messaging
Database
Mode
Repository
RADIUS
Server
NAS
Migration
Windows GINA
Appliance
OATH
Config Sync
Reporting
User Administration
Save Configuration
Upload Email Images
Administration Guide
Logout
RADIUS>NAS
Please enter the details for any RADIUS network access servers. A NAS
NAS:
Juniper
Netscaler
CiscoASA
Rob
Watchguard
Lisbon_Forti_300C
New Entry
Apply
Reset


Swivel Configuration
What's My IP Address?
Seguro | https://demo.swivelcloud.com:8080/sentry/config/radius/nas
swivelsecure
Status
Log Viewer
Server
Policy
Logging
Messaging
Database
Mode
Repository
RADIUS
Server
NAS
Migration
Windows GINA
Appliance
OATH
Config Sync
Reporting
User Administration
Save Configuration
Upload Email Images
Administration Guide
Logout
RADIUS>NAS
Please enter the details for any RADIUS network access servers. A NAS is
NAS:
Juniper
Netscaler
CiscoASA
Rob
Watchguard
Lisbon Forti 300C
Identifier: CheckPoint Dev
Hostname/IP: 89.114.238.196
Secret:
Group: ---ANY---
EAP protocol:
Authentication Mode:
Vendor (Groups): None
Change PIN warning: No
Two Stage Auth: No
Allow blank password at Stage One: No
Send Security String after Stage One: Yes
Even if User has Valid String: Yes
Check password with repository: No
Push Enabled: No
Authenticate non-user with just password: No
Username attribute for repository:
Allow alternative usernames: No
Alternative username attributes:
OTC timeout (mins): 0
Internal IP ranges:
Send username in challenge: No
New Entry
A aguardar por demo.swivelcloud.com

8 Testing

With the changes in place, when a user accesses the Gaia portal the will see the modified login page.

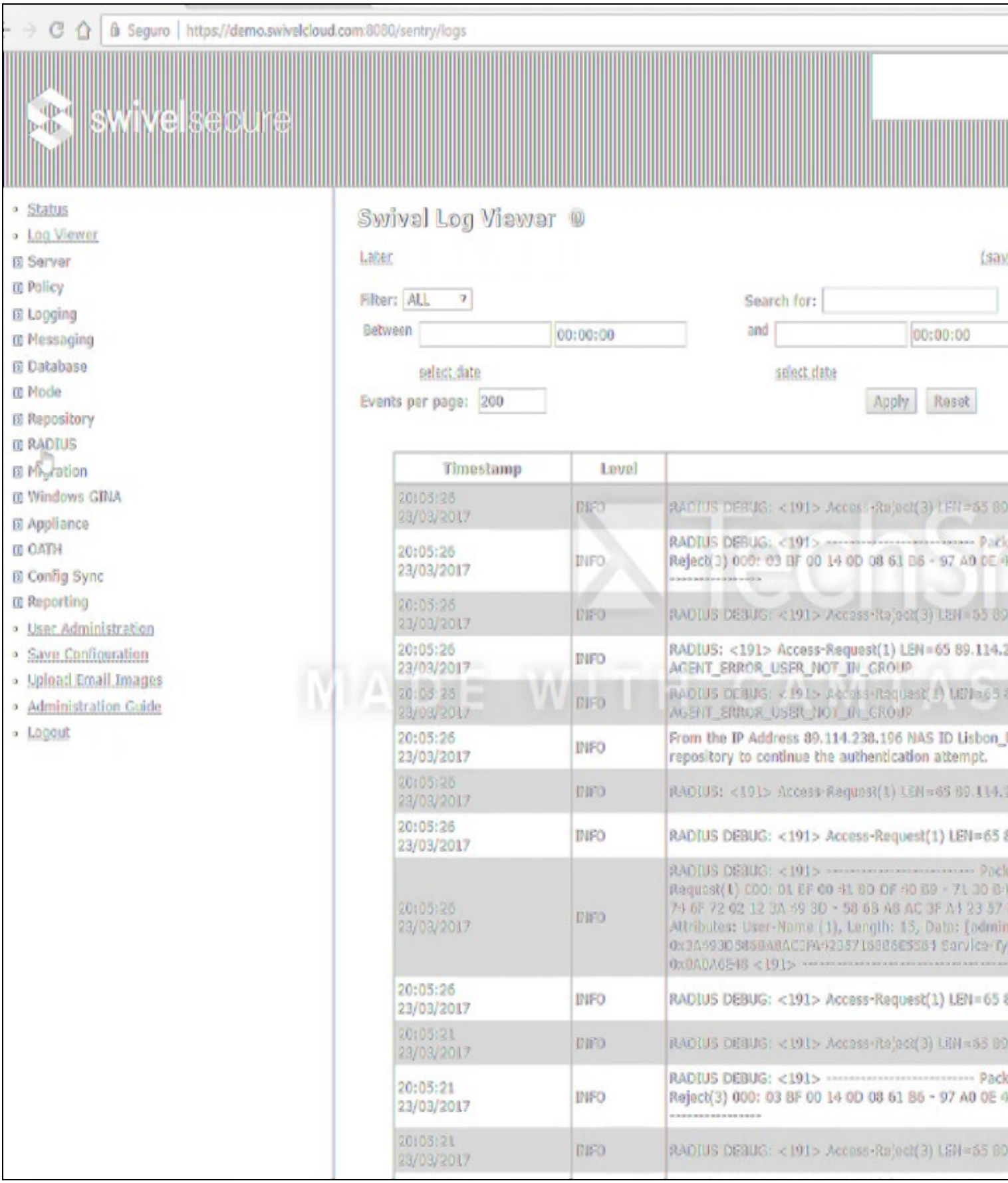


After entering their username and either tabbing away from the username field of clicking the TURing button they will be presented with a TURing image. The PINsafe log should record a session start for that user.

The user can then use their PIN to extract their one-time code and enter this to authenticate. The PINsafe log show record the RADIUS dialogue associated with this authentication.

9 Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.



10 Additional Information

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com

11 MobileIron Integration

AuthControl Sentry/Cloud to MobileIron

Integration Notes

12 Overview

Swivel Secure can provide strong and two factor authentication to the Mobile Iron. AuthControl Sentry is a linux based IdP for SAML federations. It is provided as on-prem or Cloud SaaS flavours, providing an adaptative authentication multifactor, managed by a system of points, depending on the factor used and the target app to access. This document outlines the details required to carry this out.

13 Prerequisites

Working MobileIron (MobileIron Sentry appliance) MobileIron Core 9.X and Connector 9.X AuthControl Sentry 4.x

14 How does it work

At App level we use conditional access to Cloud SaaS federated with SAMLv2. The Federated Identity works in 3-way trust with Access between Identity Provider (IDP), Service Provider (SP) and the Access provided by MobileIron AdminPortal/Access Gateway.

15 SwivelSecure Configuration

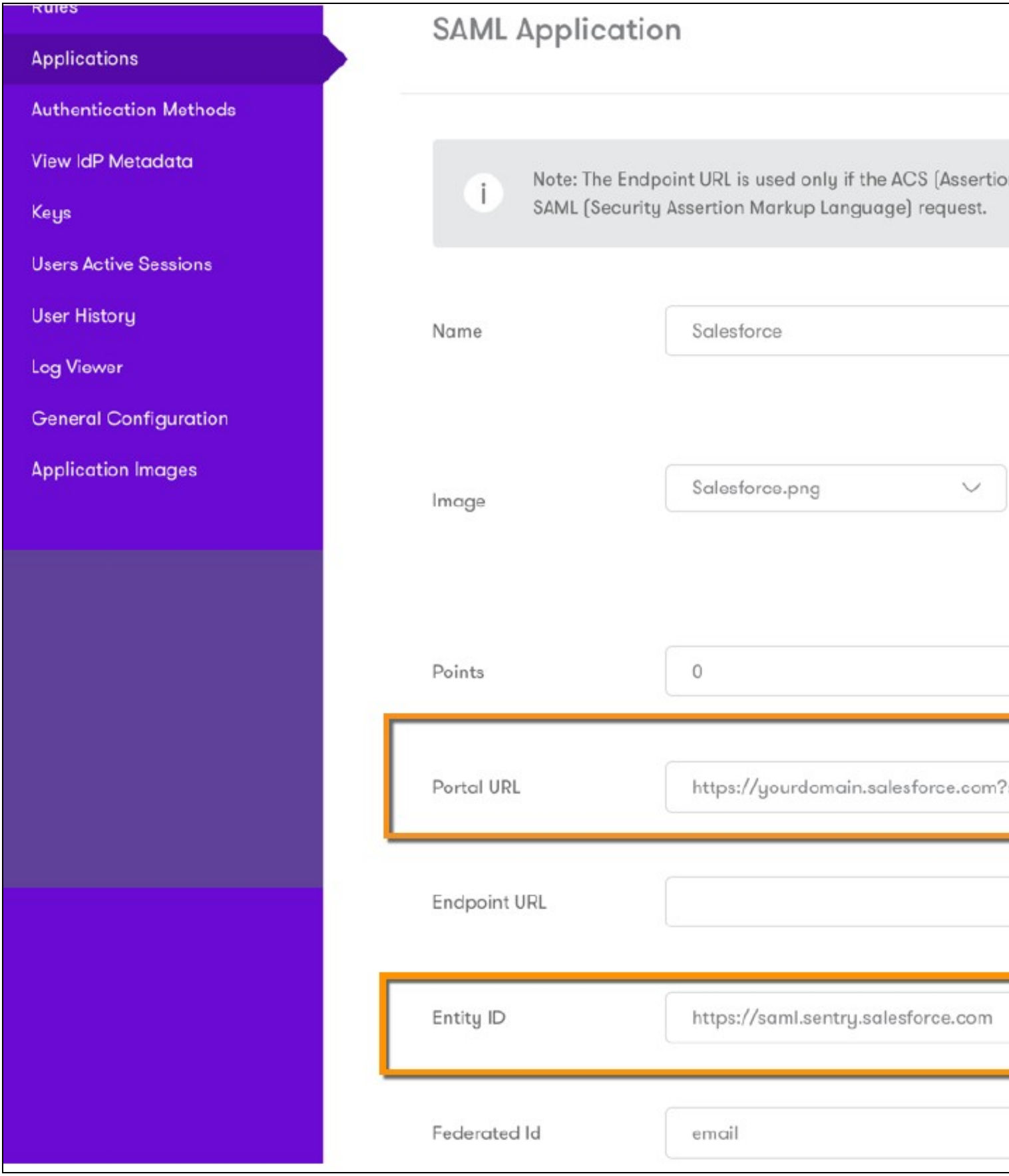
15.1 Enabling Standard Federation - Sales Force

The standard federation involves just this 3 fields:

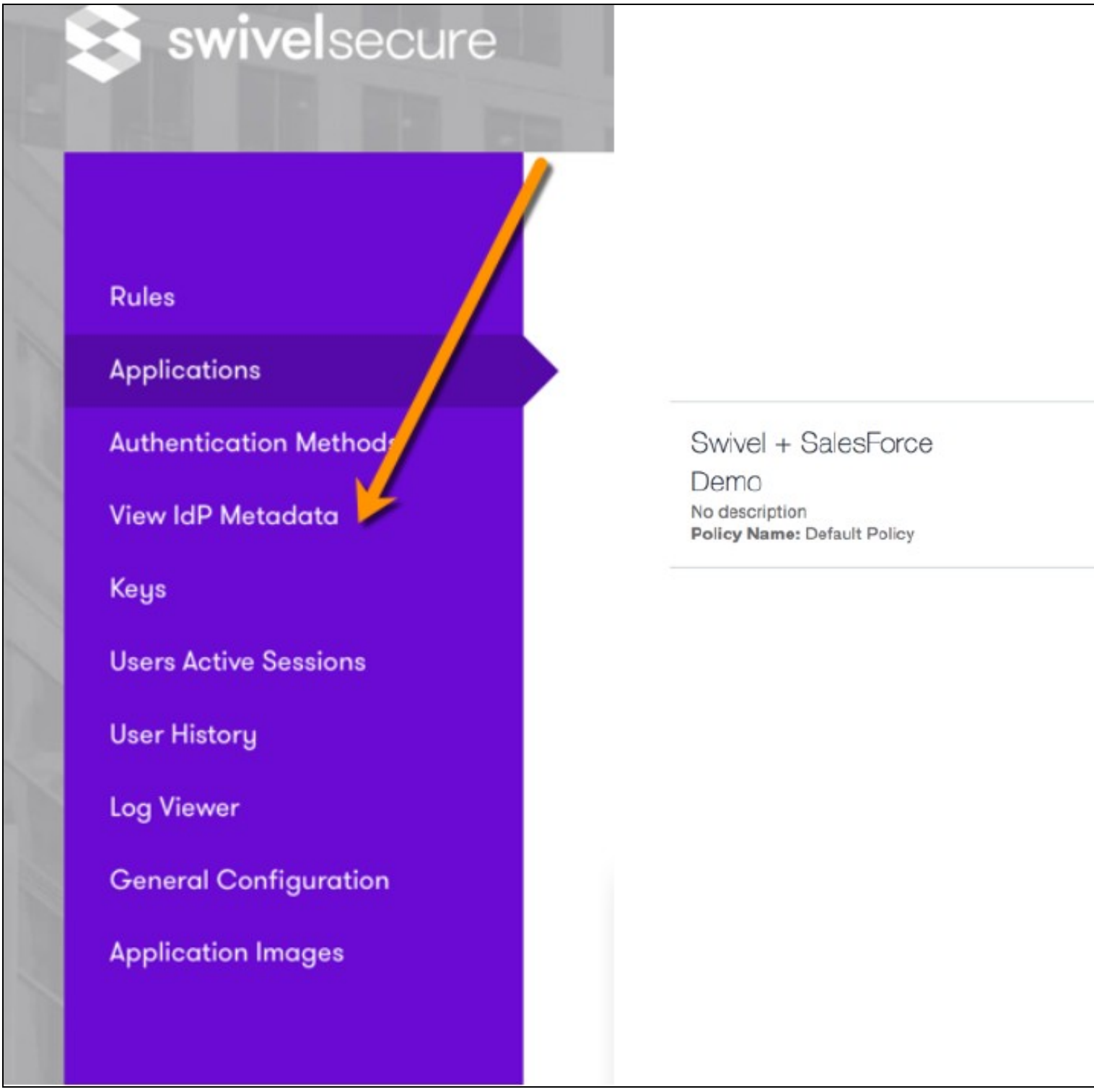
- Portal URL: (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On

Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain.

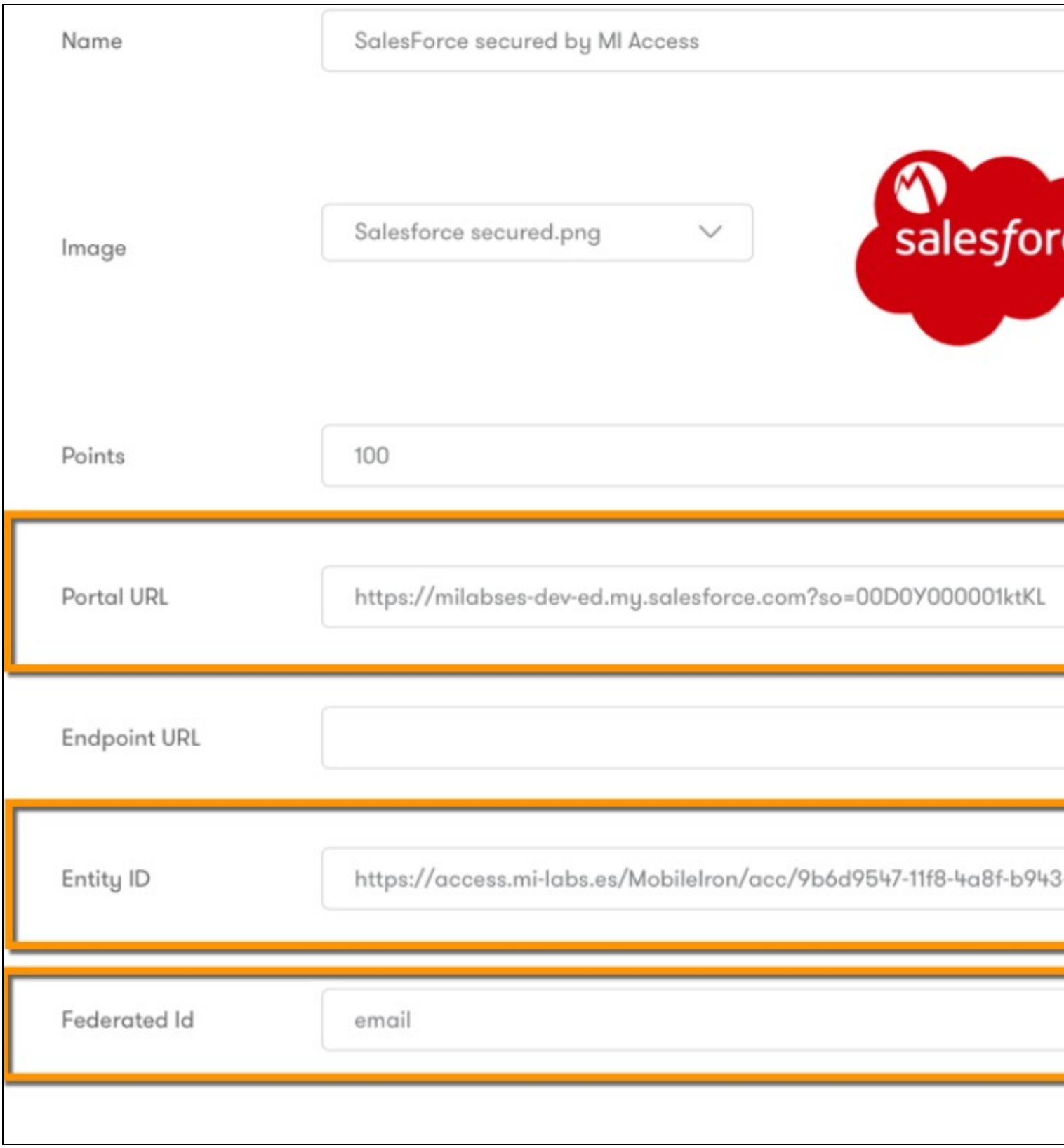
- Entity ID:, Reflected on SalesForce SSO configuration for My Domain
- Federeated id: That needs to match with the attributed defined on Salesforce.com and Swivel



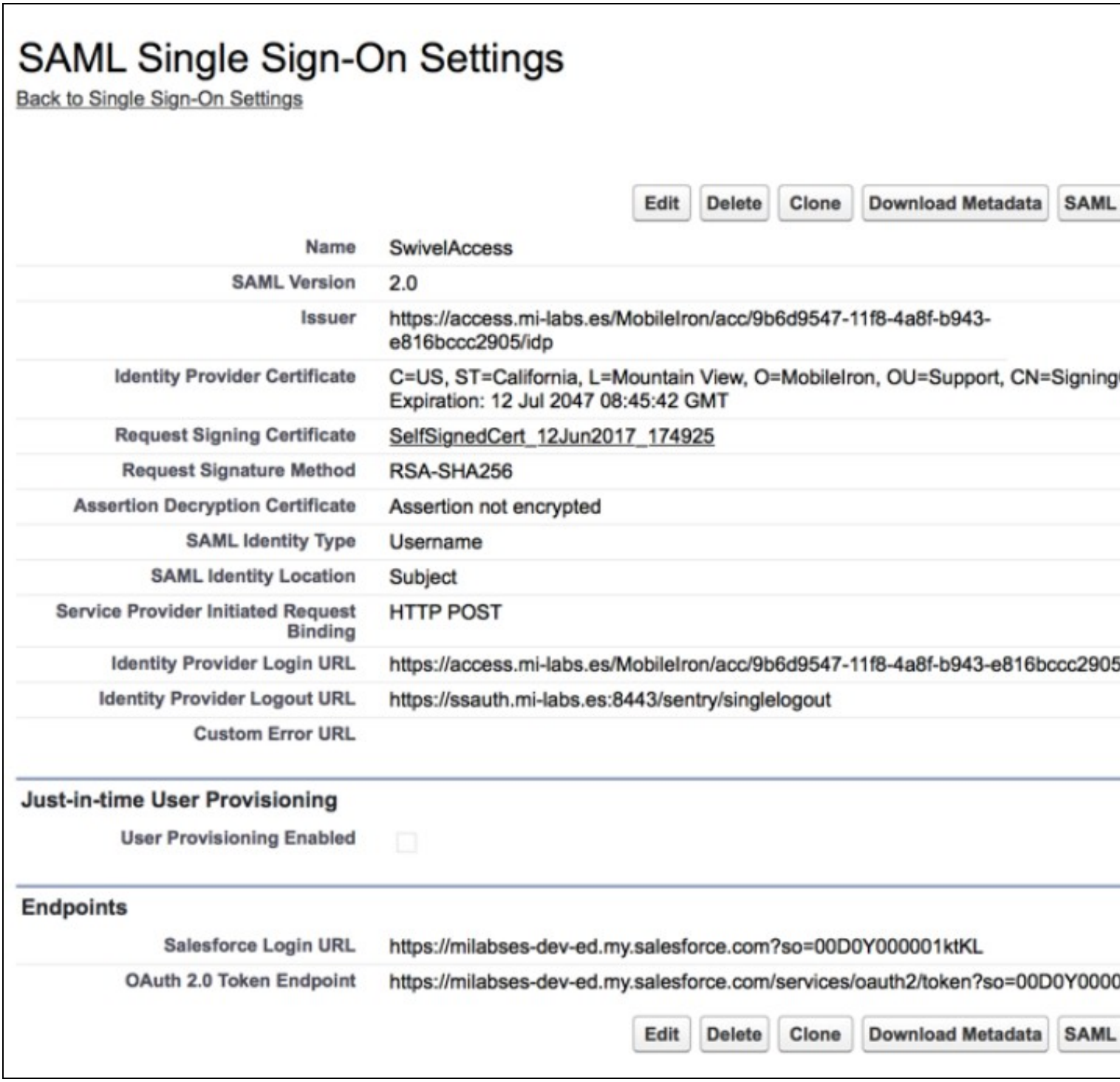
Once that we have a working federation from AuthControl Sentry and the SP, (in the example we will use SalesForce), this is just a standard SalesForce and Custom IdP federation on MI Access console, as the MFA part from Swivel will be triggered once the MI Access has approved the connection. AuthControl Sentry provides a metadata url to quickly get the XML from IdP. It uses POST method for federation.



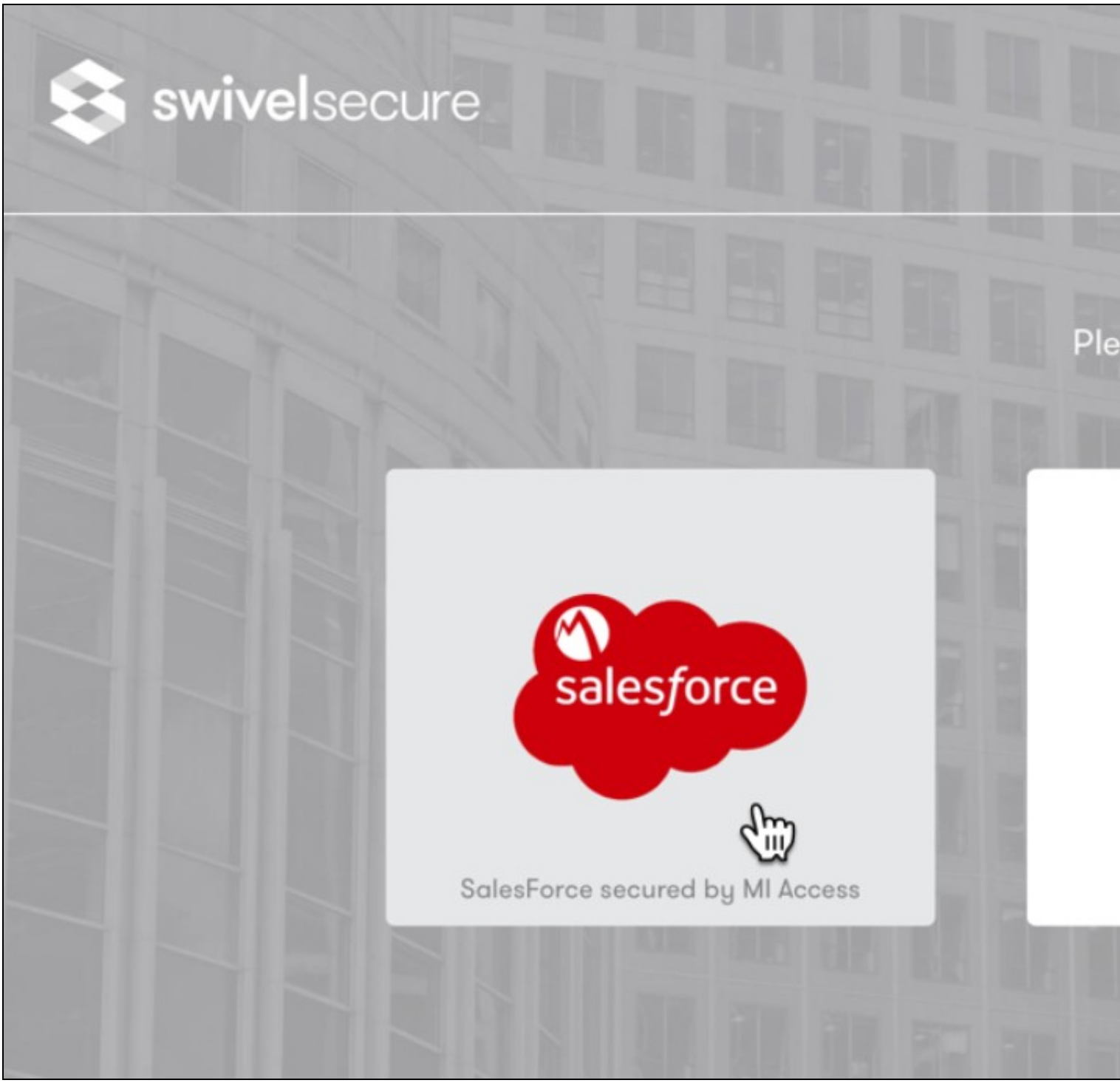
SAML Customization of Mobile Iron settings, Portal URL, Entity ID and Federated ID:



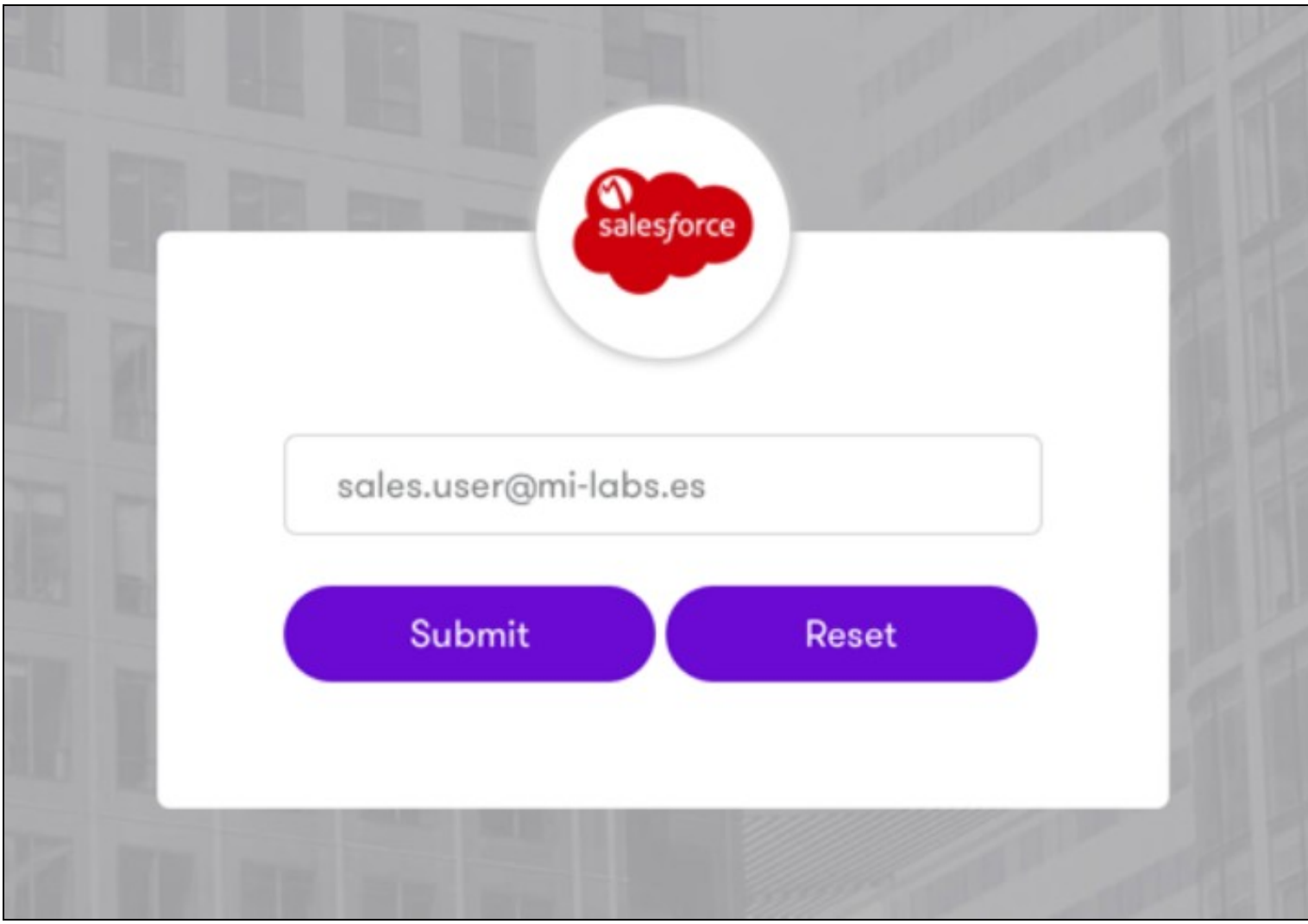
SAML Customization in the Sales Force Side. Settings for Mobile Iron.



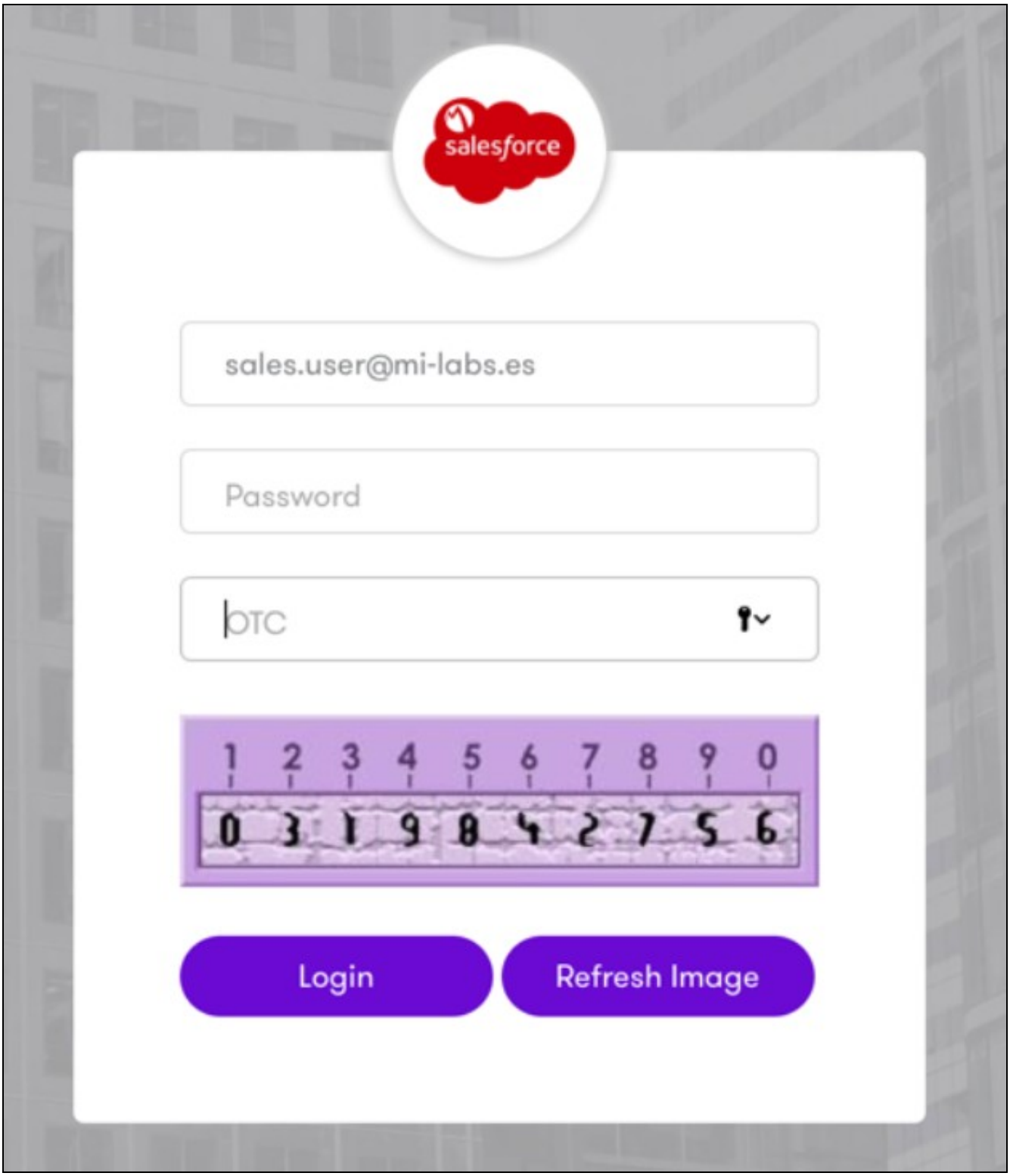
After the application settings definitions have been applied the aplications are available in AuthControl Sentry's web portal.



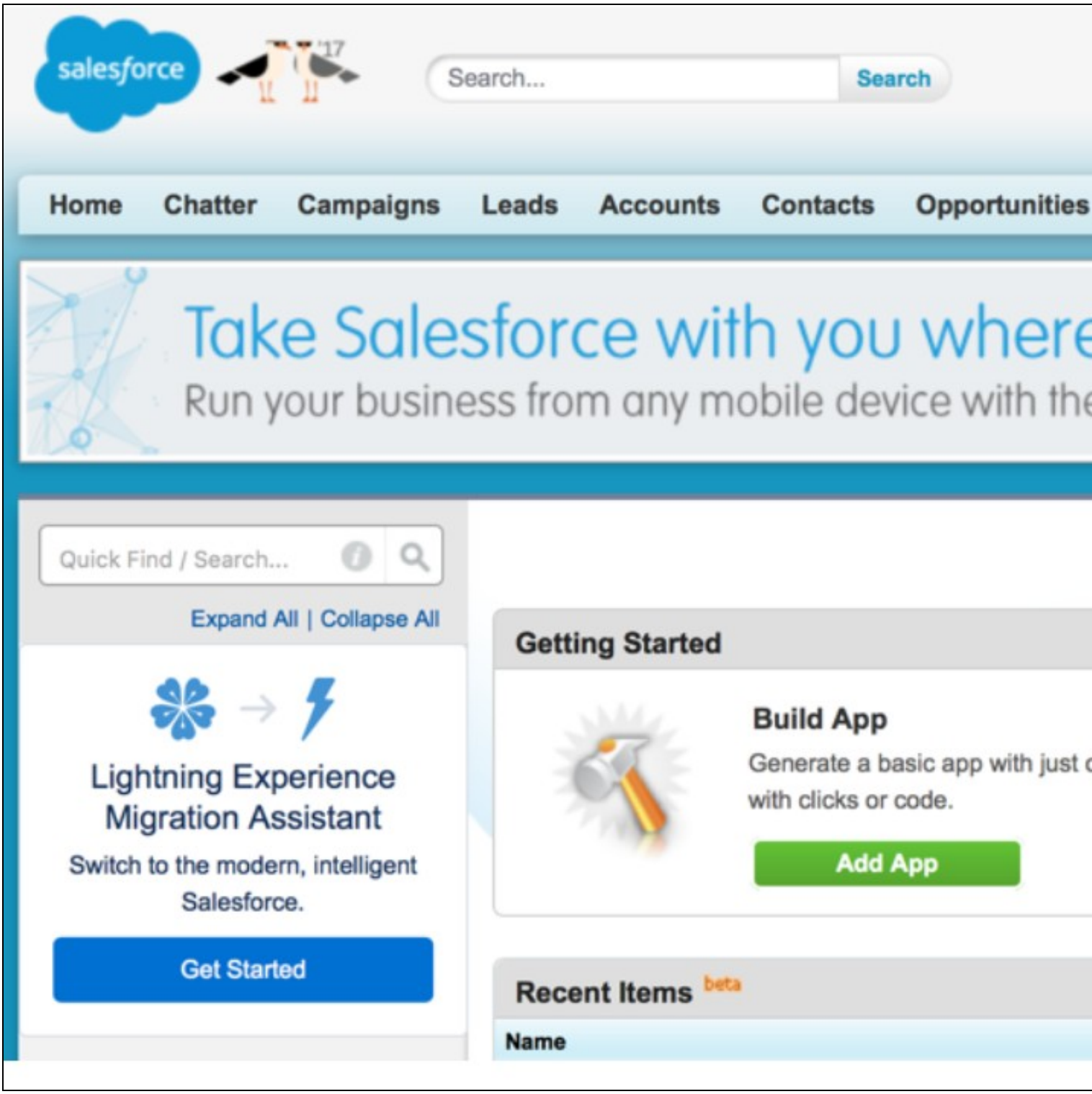
User Login in Authcontrol Sentry with SalesForce using the MI Account



SSO for SalesForce using Mobile Iron and Turing image from SwivelSecure. This means that the user logs in using the Swivel Secure credentials, by the selected method (in this case Turing image) into the Sales Force (without the need of using Sales Force Credentials).

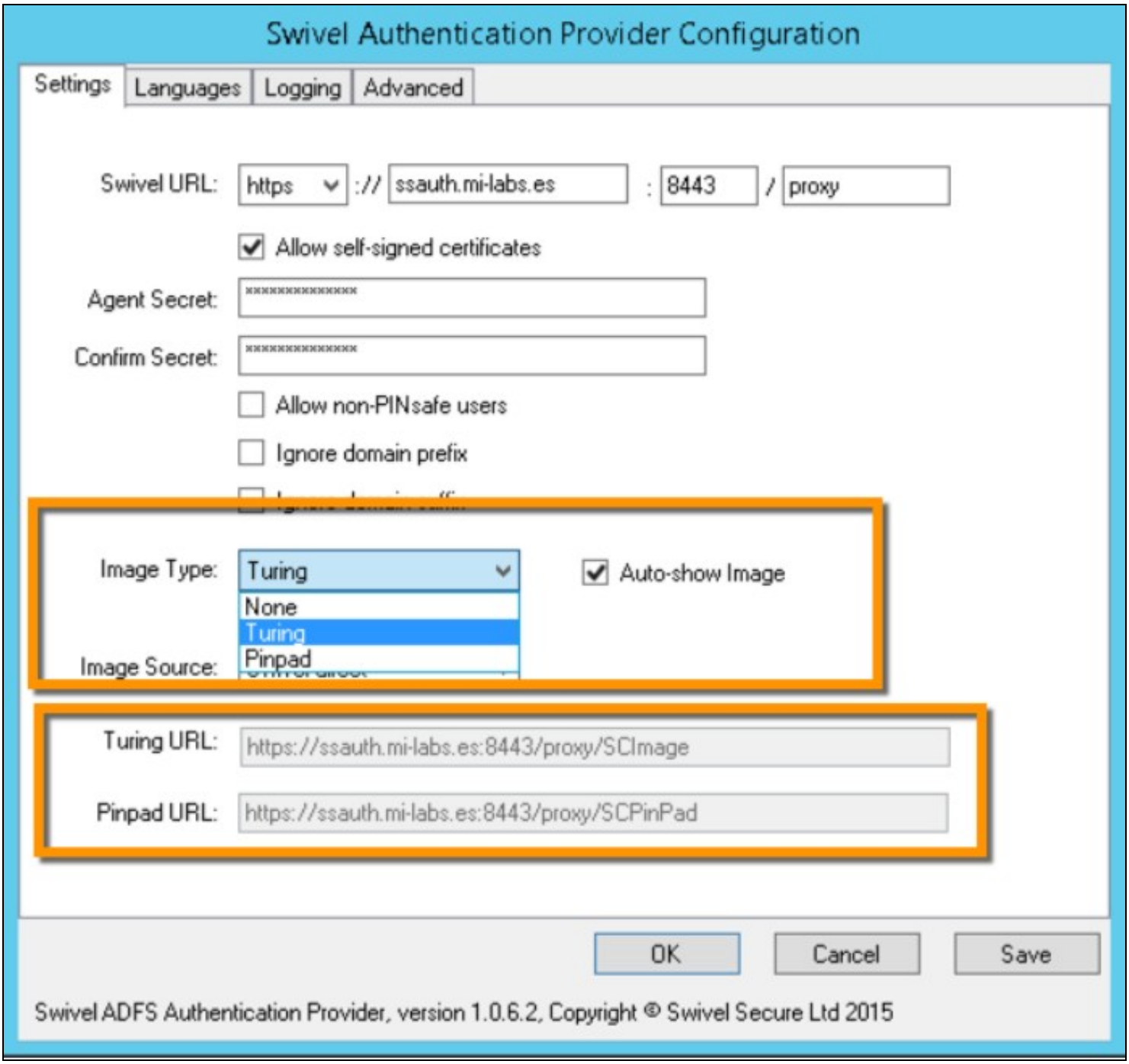


Successfull login in Sales Force.



15.2 Enabling Standard Federation - Office 365

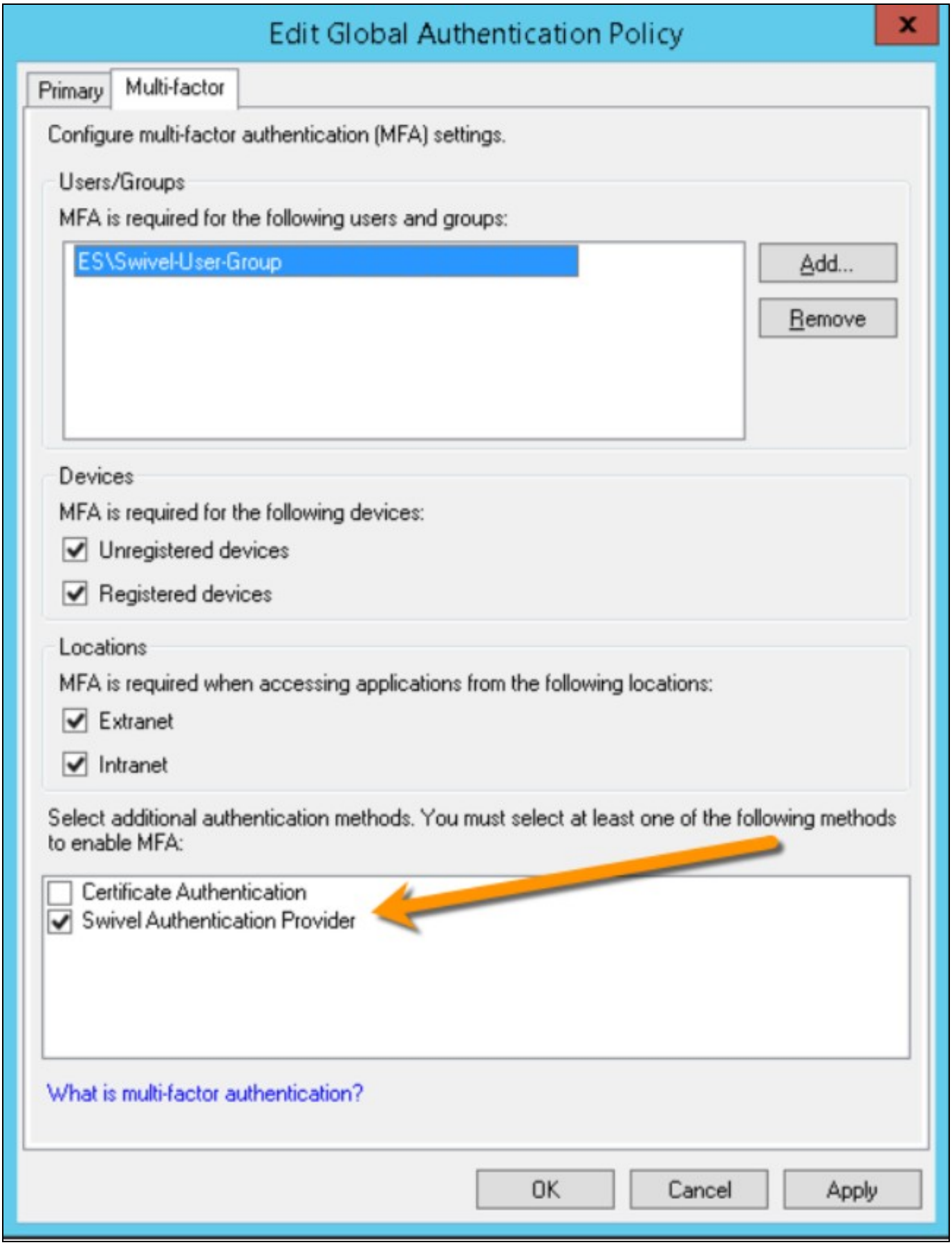
In the case of Office365, AuthControl requires that the main federation must be performed with ADFS. On a working federation, a complement has to be installed on ADFS 3.0 server.



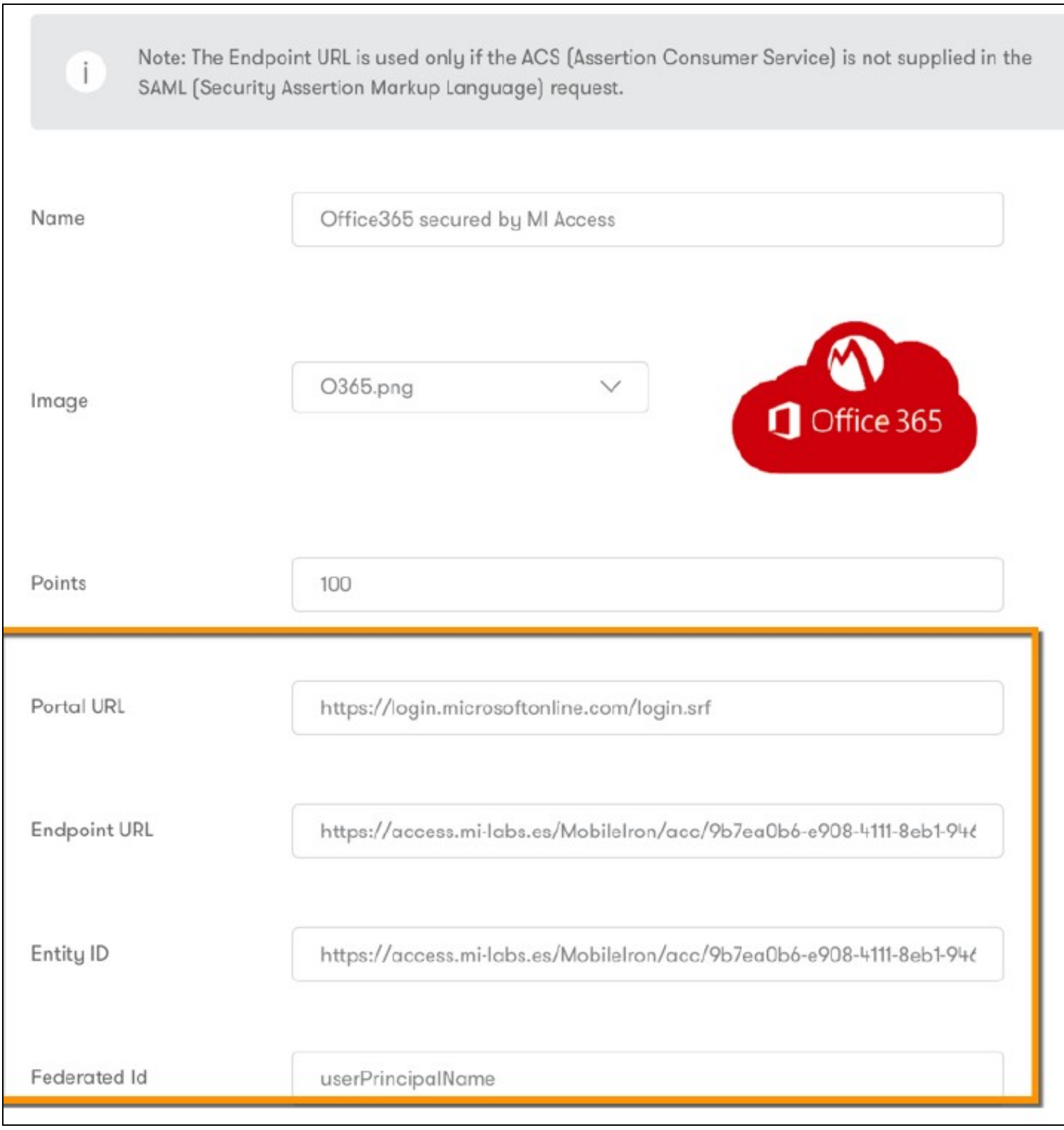
There?s a couple of choices depending if the customer is using ADFS Proxy servers or not.

This plugin installs Swivel Secure product as an MFA to be applied via ADFS Authentication Policy Settings.

Set AuthControl Sentry / Swivel Secure as Authentication Provider



On AuthControl Sentry side, we will create an Application configuration with MI Access, IdP and Office365 endpoints:



This way, ADFS will require PINPAD or Turing image in order to validate and access Office365, in addition to ADFS primary authentication policy.

MI LABS ES Login

Welcome ES\office.user

For security reasons, we require additional information to verify your account

OTC:

refresh

Continue

16 Related Articles

- ADFS configuration

https://kb.swivelsecure.com/w/index.php/Microsoft_ADFS_3_Authentication

17 Additional Information

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com